CERTIFIED COPY OF PRIORITY DOCUMENT

מדינת ישראל
STATE OF ISRAEL

istry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

to certify that annexed
s a true copy of the
ts as originally
with the patent
of which
ecified on the
ex.

זאת לתעודה כי רצופים
בזה העתקים נכונים של
המסמכים שהופקדו
לכתחילה עם הבקשה
לפטנט לפי הפרטים
הרשומים בעמוד הראשון
של הנספח.

This 15-01-2001 היום

רשם הפטנטים

Commissioner of Patents

נתאשר
Certified

חוק הפטנטים, תשכ"ז - 1967
PATENTS LAW, 5727-1967

לשימוש הלשכה
For Office Use

מספר: Number	134047
תאריך: Date הוקדם / נדחה Ante / Post-dated	14 -01- 2000

בקשה לפטנט
Application for Patent

אני, (שם המבקש, מענו – ולגבי גוף מאוגד - מקום התאגדותו)
I, (Name and address of applicant, and, in case of a body corporate, place of incorporation)

אי. סי. איי טלקום בע"מ
רחוב הסיבים 30
פתח תקווה 49517
(חברה ישראלית)

ECI TELECOM LTD.
30 Hasivim Street
Petach Tikva 49517
(an Israeli Company)

הממציא(ים): Inventor(s):

בעל אמצאה מכח הדין Owner, by virtue of Right of Law
ששמה הוא: of an invention, the title of which is:

(בעברית) (Hebrew)
שיטה לבחירת סוגי ערוצי תקשורת ברשת רב שכבתית ומערכת בה משתמשים בשיטה זו

(באנגלית) (English)
METHOD FOR SELECTING THE TYPE OF COMMUNICATION CHANNELS IN A MULTI-LAYERED NETWORK AND SYSTEM USING SAME

מבקש בזאת כי ינתן לי עליה פטנט. Hereby apply for a patent to be granted to me in respect thereof

• בקשת חלוקה Application for Division	• בקשת פטנט מוסף - Application for Patent of Addition	• דרישת דין קדימה Priority Claim		
מבקשת פטנט from Application	• לבקשה/לפטנט to Patent/Application	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
No. _____ מס' _____ dated מיום	No. _____ מס' _____ dated מיום			
• יפוי כח: כללי/מיוחד - רצוף בזה/עד יוגש P.O.A.: general/specific - attached/to be filed later Has been filed in case _____ הוגש בענין				
המען למסירת הודעות ומסמכים בישראל Address for Service in Israel ד"ר גיל אינגל אי. סי. איי טלקום בע"מ ת.ד. 3083 פתח תקווה 41930 ECIP/F006/IL				
חתימת המבקש Signature of Applicant		היום 13 בחודש January שנת 2000.		
				לשימוש הלשכה For Office Use

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם במספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application, the particulars of which are set out above.

• מחק את המיותר Delete whatever is inapplicable

שיטה לבחירת סוגי ערוצי תקשורת ברשת רב שכבתית ומערכת בה
משתמשים בשיטה זו

METHOD FOR SELECTING THE TYPE OF COMMUNICATION CHANNELS IN A MULTI-LAYERED NETWORK AND SYSTEM USING SAME

ECI TELECOM LTD.

אי.סי.איי טלקום בע"מ

Field of the Invention

The present invention relates to the management of telecommunication networks, and in particularly to the management of optical networks.

Background of the Invention

Telecommunication systems comprising a number of optical transmission channels are known in the art. Unfortunately, these systems suffer occasionally from a fault occurring in one of these channels, e.g. due to failing components. Therefore, a protection channel is usually incorporated in such systems, allowing the diversion of transmitted communication to a non-failing channel, the protection channel. Traditionally, monitoring the performance in these telecommunication systems was done while incorporating various alarm conditions. Such alarm conditions alerted a human operator when certain events e.g. a loss of signal or error rates that had exceeded pre-defined thresholds were detected. In response to such an alarm, the operator would manually switch to a redundant path in the network, allowing the communication to continue.

At a later stage, conventional fiber optic fibers have implemented 1:1 redundancy for the optical channels in a network, with a certain amount of automatic switching. In these systems, when a loss of signal (to be referred to hereinafter as "LOS") or alarm indication signal ("AIS") conditions were noted in a channel connecting a first location to a second location, a diversion of the transmission to the available redundant path was made. This diversion enables the transmission of data between these first and second locations to continue.

US 4,646,286 discloses a system wherein a protection switch is effected by detecting a channel failure at receiving end. Thereafter, a protection request is transmitted on the return channel to the transmission end. This request is then used in a controller for the channel to activate a switch to the corresponding protection channel.

However, since this solution requires doubling both the cabling and the input/output ports as compared with those required to carry traffic, such a solution is quite expensive.

However, when dealing with a multi element and multi layered networks, one that combines for example a number of optical rings, one of the problems arising is how to manage effectively such a network, and how to differentiate between main paths and protective paths, when those all the paths are derived from the combination of the various elements and as such could well be that a segment that was defined as a protective path for a stand alone sub-network, could serve as a main path for the complete network.

Some work has been carried out in various telecommunication standardization bodies in an effort to define what would be required for network management. This work is summarized in ETSI publication: TS 101 010 V1.1.1 (11/1997) entitled "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network Protection Schemes; Interworking: rings and other schemes", and in SIF document SIF-IM-9807-117], both of which are incorporated herein by reference.

Summary of the Invention

It is an object of the present invention to provide An effective method for the management of a multi layered optical telecommunication network.

It is yet another object of the present invention to provide a network management element and a system comprising such an element wherein the management of the network is carried out at the network level rather than on a layer by layer basis or on an element by element basis.

Other objects of the invention will become apparent as the description of the invention proceeds.

In accordance with the present invention there is provided a method for managing a multi-layered network wherein a selection criterion is used for determining a main transmission path as distinct from a protective path.

According to a preferred embodiment of the invention, the selection criterion is based on the definition of the shortest available transmission path and determining said path as the main path. More preferably, in accordance with the present invention, the selection criterion is based on the position of the various switches located along the available transmission paths and is determined in accordance with the default position or the initial position of these switches, or a combination of the two.

According to still another embodiment of the invention, the multi-layered network is an SDH network that comprises a at least two different layers. Each such layer is selected from the group consisting of optical channel layer, multiplexed section layer, SDH high order layer, SDH low order layer, ATM layer and the like.

Similarly, the present invention is also provided for the case where the multi-layered network is a SONET network that comprises a at least two different layers. Each such layer is selected from the group consisting of optical channel layer, VT layer, STC layer, Section layer, line layer, ATM layer and the like.

By another embodiment of the present invention the network to be managed in accordance with the method provided comprises at least two different layers, each of which has its own independent protection path. After applying a selection criterion similarly to the one described above, the main path can be determined for the network, and similarly the path that will be used as the protective path.

According to still another embodiment of the invention, the protective path can be a non-continuous path and to comprise at least two segments that are not directly connected to each other.

Examples for this embodiment can be when the at least two different layers are optical channel layer and multiplexed section layer, or alternatively optical channel layer and VT layer, or any other combination of a multi-layer arrangement described.

According to another aspect of the present invention there is provided a network management element for managing the operation of a multi-layered telecommunication network and is operative to determine a main transmission path in the network to be managed as distinct from a protective path therein.

According to an embodiment of this aspect of the invention the network management element is adapted to operate in an SDH network or in a SONET network.

By still a further embodiment of the invention there is provided a system comprising a network management element characterized in that the main communication transmission path as well as the protective paths are defined at the network level rather than on a layer by layer basis or on an element by element basis.

Brief Description of the Drawings

Figs. 1 to 3 illustrate various embodiment of diverse path protection.

Fig. 4 illustrates a case with a single point of failure.

Fig. 5 demonstrates a Dual Ring Interworking (DRI).

Fig. 6 illustrates an embodiment of the present invention wherein the main (working) path is determined according to the shortest path found in the network.

Fig. 7 illustrates an example of another embodiment of the present invention wherein the main (working) path is determined according to the switch default position in the network.

Fig. 8 demonstrates a further embodiment of the invention wherein a protective path comprises a number of segments.

Detailed Description of the Invention

The following description of network management including the requirements associated therewith are described as an example of the present invention.

I. Requirements:

Protection Schemes ("PS")

An SNC may be unprotected or protected. Different protection schemes are available to provide protection for SNCs.

In the following description the term "mandatory" will be used hereinafter to denote a feature that must be supported by all EMS and NMS, and the term "optional" will be used hereinafter to denote a feature that may be supported only by part of the EMSs.

The following is a description of the requirements for these cases.

Requirement PS:1: The following Protection Schemes will be supported by the interface:

LO-VC SNC-P,

HO-VC SNC-P,

MS SPring and MS-Linear;
Optical Channel Protection and
Unspecified.

Requirement PS.2: The interface will allow the NMS to query the Subnetwork objects of an EMS to determine the protection schemes supported. The EMS will report all schemes that are possible even if they may not be supported for every SNC.

Requirement PS.3: The interface will allow the NMS to specify the desired protection scheme to implement when provisioning an SNC.

The EMS will attempt to fulfil the specified scheme. If the specified scheme cannot be applied the EMS may choose to use a different protection scheme.

Requirement PS.4: The interface will allow the NMS to query the EMS to determine the protection schemes, if any, that exists for an existing SNC.

Requirement PS.5: The description of the protection scheme of an SNC will allow for layered protection schemes where more than a single protection scheme is providing protection. An enumeration of all relevant protection schemes will be contained in the protection scheme attribute.

No differentiation will be made between inter layer and intra layer schemes. This means that the protection scheme attribute is the union of all schemes used without indicating if they are applied concurrently, chained or even if there are gaps with no protection scheme applied for portions of an SNC.

Requirement PS.6: The interface will support a Traffic Availability indication that measures the degree

to which the traffic is protected. The following values for the Traffic Availability will be supported:

- Unprotected,
- Single Point of Failure (SPoF) – There exists a common fiber or NE besides the endpoints. (see figure 1 for and example.)
- Diverse Protection - No Single Point of Failure exists within the SNC. The endpoints may for a SPoF. (see figures 1-3 for example of diverse routed, exclusive merge SNCs)
- Highly Protected – Indicates a higher level of protection than is possible by simple diverse routing. Multiple rings can each experience a single ring failure without affect the robustness of either inter or intra ring traffic. Typically this would be achieved by using Dual Ring Interworking ("DRI") where the proper use of links enhances survivability over that offered by simple diverse routing. This is equivalent to the Level 3 availability of ETSI TS 101 010. (See Figure 5 for an example of such DRI.
- Unspecified – protection of the SNC exists but it is not possible to determine the exact value.

Requirement PS.7: The interface will allow the NMS to specify the desired protection scheme to implement when provisioning an SNC.

Requirement PS.8: The interface will allow the NMS to query the EMS to determine the protection scheme, if any, that exists for an existing SNC.

Requirement PS.9: The interface will allow the NMS, when creating an SNC, to specify more than two endpoints according to the SNC to be created. Each endpoint will

have an indication to state if they are for the protection path or the main path.

Requirement PS.10: The ProtectionEffort (values are BestEffort or Exact) attribute will relate to the TrafficAvailability attribute. The BestEffort attribute does not affect the ProtectionScheme used by the EMS.

An unprotected SNC will not be created if the EMS is unable to provide protection of any type when requested to create a protected SNC with BestEffort indicated.

Requirement PS.11: The NMS will be able to determine the current active path of a SNC. This dynamic data is not an attribute of an SNC but rather indicates, per protection switching point, the current switch position. This requirement is for all types of protection implemented including equipment protection, MS-Linear and VC-SNCP protection

Point to Multi Point SNC and its Protection

Point to Multi Point ("P2MP") SNC may be represented as multiple SNCs or as single SNC. The single SNC model is appropriate when the subnetwork is a mesh. In a mesh topology subnetwork, individual path segments may be common to several Add Drop TP pairs. The use of a single SNC to represent the complete P2MP SNC eliminates the need to maintain links to the different P2MP components. (Note: When multiple SNC are used to represent a single P2MP SNC the responsibility to prevent the deletion of common resources when deactivating an SNC remains to be addressed.). The following is a description of the requirements for these cases.

Requirement MP.1: The interface will allow the NMS to specify the creation of multiple Drop endpoints for a Unidirectional Point to Multi Point SNC.

Requirement MP.2: The interface will allow the NMS to add or remove a drop leg to an existing Point to Multi Point SNC.

Requirement MP.3: The interface will support the representation of Point to Multi Point SNCs across the interface.

Requirement MP.4: The interface will support the creation of Protected Point to Multi Point SNCs. The EMS will attempt to have every endpoint protected. If the EMS is unable to provide protection for all endpoints, the SNC will still be created, as long as one A-Z endpoint pair is protected, and the TrafficAvailability indicator will be set to SinglePointOfFailure to indicate that some endpoints are not protected.

Requirement MP.5: The interface will support a query to find the Protection scheme used for Point to Multi Point SNCs across the interface.

II. Object Model ("OM"):

OM.1 Route Object

The following attributes of the Route Object will be made:

*Attribute Name:	Working
Attribute Description:	Assigned by EMS upon creation of a sub-network connection; may not be empty; contains ordered sequence of CTP names For a protected SNC the name list will include only the CTPs that are used for the initial transmission path end to end. CTPs that are in the SNC for use only as part of the protection mechanism are not included in the working path. (This the case for SNCP and Dual Ring Interworking) For routes that perform multicast corss-connects (one CTP transmits to more than one CTP within a ME) the following method will be used for relying the path of the SNC: Starting with an A-EndPoint the list will contain the ordered sequence of CTP names to a Z-EndPoint. For all multi-cast cross connects existing in the list the CTP that is the source of the multicast will be added to the list again. To the list will then be added all the CTPs from the multicast CTP that form an ordered sequence of CTP names to a Z-EndPoint that has not previously been visited. All CTPs that form the source of a multicast cross connect will appear in the list the same number of times as the number of edges that are connected to it. If multiple A-Endpoints exist then the

	path starting from the additional A-Endpoints are appended to the end of the Name list. Resources that are common to Working and Protected paths appear in each attribute's NameList.
*Type/Syntax:	NameList
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value	N/A
*Invariant?	Y

*Attribute Name:	Protected
Attribute Description:	Assigned by EMS upon creation of a sub-network connection; may be empty; contains ordered sequence of CTP names. All CTPs that are not in use by the initial SNC transmission path but are allocated as protecting for the working path are included in this NameList. These CTP in the NameList s may form non-contiguous fragments. Resources that are common to Working and Protected paths appear in each attribute's NameList. For routes that perform multicast cross-connects (one CTP transmits to more than one CTP within a ME) the following method will be used for relying the path of the SNC: Starting with an A-EndPoint the list will contain the ordered sequence of CTP names to a Z-EndPoint. For all multi-cast cross connects existing in the list the CTP that is the source of the multicast will be added to the list again. To the list will then be added all the CTPs from the multicast CTP that form an ordered sequence of CTP names to a Z-EndPoint that has not previously been visisted. All CTPs that form the source of a multicast cross connect will appear in the list the same as the number of edges that are connected to it.

	If multiple A-Endpoints exist then the path starting from the additional A-Endpoints are appended to the end of the Name list.
*Type/Syntax:	NameList
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value	N/A
*Invariant?	Y

OM.2 SNC Object

SNC object requires the following new operations:

*Operation Name:	GetSupportedProtectionSchemes
Operation Description:	The operation is used to get a list of all protection schemes that the EMS supports. For a particular SNC it is valid that not all protection schemes will be available. If the EMS is unable to determine the schemes supported then scheme of Unspecified will be returned.
Precondition(s):	None
*Parameter Name(s):	None
Parameter Description(s):	NA
*Parameter Type(s):	NA
Return Type Description(s):	ProtectionSchemeList

*Return Type/Syntax:	List of enumerated type protectionScheme
Postcondition(s):	None
*Operation Exception(s):	

*Operation Name:	AddDropLeg
Operation Description:	If the existing SNC is in the Pending state then the drop leg will be created but not activated. If the existing SNC is in the Partial state then the drop leg will be created and activated; the resulting SNC will be in the Partial state. If the existing SNC is in the Active state the resulting SNC may be the Partial state or Active state.
Precondition(s):	An existing unidirectional or point-to-multipoint SNC.
*Parameter Name(s):	SNCid, newZendpoint
Parameter Description(s):	SNCid - the id of the SNC to be modified. new z-EP - the CTP that is a new drop leg of the SNC.
*Parameter Type(s):	SNC name, TPPlan
Return Type Description(s):	SNC
*Return Type/Syntax:	Subnetwork
Postcondition(s):	The resulting SNC will include a new

	leg of the SNC to the Z-endpoint. The state of the SNC may be Pending, Partial or Active. The protectionLevel will be set to point-to-multipoint.
*Operation Exception(s):	

*Operation Name:	deleteDropLeg
Operation Description:	Deactivates and deltes a drop leg of a point-to-multipoint SNC.
Precondition(s):	The SNC has at least two drop legs.
*Parameter Name(s):	SNCid, exisitingZendpoint
Parameter Description(s):	SNCid - the id of the SNC to be modified. exisitngZ-EP - the CTP that is a drop leg of the SNC to be deleted.
*Parameter Type(s):	SNC name, TPPlan
Return Type Description(s):	None
*Return Type/Syntax:	None
Postcondition(s):	The protectionLevel will be set to unidirectional or point-to-multipoint as appropriate.
*Operation Exception(s):	

The Subnetwork operations require the following changes:

*Operation Name:	createSubnetworkConnection
Operation	Create a new Subnetwork Connection.

Description:	
Precondition(s):	None
*Parameter Name(s):	1) aEndTPPlanList 2) zEndTPPlanList 3) directionality 4) protectionMode 5) protectionEffort 6) protectionScheme 7) connectionMode 8) timeslot 9) userLabel 10) ownerLabel
Parameter Description(s):	1) A list of the names of A-end connection termination points and associated attribute-value pairs for transmission parameters. There is also an associated Main/Protection/Both indicator that determines which path the endpoint is terminating. There will be multiple endpoints in the A-endpoint list if the SNC does not have a single A-endpoint entry into the subnet. 2) A list of the names of Z-end connection termination points and associated attribute-value pairs for transmission parameters. There is also an associated Main/Protection/Both indicator that determines which path the endpoint is terminating. There will be multiple endpoints in the Z-endpoint list if the SNC does not have a single

	Z-endpoint. This is the case for point-to-multipoint SNC and for some instances of protected SNC. 3) Directionality of the subnetwork connection. 4) Protection mode of the subnetwork connection Note: in SNC this is marked as "protectionLevel". 5) protectionEffort is either "bestEffort" or "exact" match 6) protectScheme is the suggested protection scheme to be used. The EMS may use any scheme. 7) Connection mode of the subnetwork connection. 8) A channel to be used by the subnetwork connection. 9) A user-friendly name to be assigned to the subnetwork connection. 10) A label of the owner of the subnetwork connection.
*Parameter Type(s):	1) in TPPlanList 2) in TPPlanList 3) in Directionality 4) in ProtectionMode 5) in ConnectionMode 6) in ProtectEffort 7) in ProtectScheme 8) in Timeslot (This is actually an inout parameter.) 9) in String 10) in String

Return Type Description(s):	The newly created Subnetwork Connection object.
*Return Type/Syntax:	SubnetworkConnection
Postcondition(s):	None
*Operation Exception(s):	1) At least 1 of the TPPlans is invalid. 2) Resource limitation. 3) A route can not be found between the specified CTPs. 4) The timeslot was not specified and there were no timeslots available for routing the SNC.

*Operation Name:	checkValidSubnetworkConnection
Operation Description:	Check whether a valid Subnetwork Connection can be created based on input parameters without actually creating it.
Precondition(s):	None
* Parameter Name(s):	1) aEndTPPlanList 2) zEndTPPlanList 3) directionality 4) protectionMode 5) protectionEffort 6) protectionScheme 7) connectionMode 8) timeslot 9) userLabel 10) ownerLabel
Parameter Description(s):	1) A list of the names of A-end connection termination points and

	associated attribute-value pairs for transmission parameters. There is also an associated Main/Protection/Both indicator that determines which path the endpoint is terminating. There will be multiple endpoints in the A-endpoint list if the SNC does not have a single A-endpoint entry into the subnet. 2) A list of the names of Z-end connection termination points and associated attribute-value pairs for transmission parameters. There is also an associated Main/Protection/Both indicator that determines which path the endpoint is terminating. There will be multiple endpoints in the Z-endpoint list if the SNC does not have a single Z-endpoint. This is the case for point-to-multipoint SNC and for some instances of protected SNC. 3) Directionality of the subnetwork connection. 4) Protection mode of the subnetwork connection Note: - in SNC this is marked "protectionLevel". 5) protectionEffort is either "bestEffort" or "exact" match 6) protectScheme is the suggested protection scheme to be used. The EMS may use any scheme. 7) Connection mode of the subnetwork connection.

	8) A channel to be used by the subnetwork connection. 9) A user-friendly name to be assigned to the subnetwork connection. 10) A label of the owner of the subnetwork connection.
*Parameter Type(s):	1) in TPPlanList 2) in TPPlanList 3) in Directionality 4) in ProtectionMode 5) in ConnectionMode 6) in ProtectEffort 7) in ProtectScheme 8) in Timeslot (This is actually an inout parameter.) 9) in String 10) in String
Return Type Description(s):	True if a valid subnetwork connection can be created and False otherwise.
*Return Type/Syntax:	Boolean
Postcondition(s):	None
*Operation Exception(s):	None

OM.3 SNC Object

The following SNC Attributes that are new:

*Attribute Name:	ProtectionScheme
Attribute Description:	Indicates the protection schemes that are used to provide protection to the SNC.

	The type Unprotected is used for SNC that have no protection implemented.
*Type/Syntax:	List of enum values from the following: • LO-VC SNC-P, • HO-VC SNC-P, • MS SPring and MS-Linear; • Optical Channel Protection • Unspecified • Unprotected
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value:	Unspecified
*Invariant?	N

*Attribute Name:	TrafficAvailability
Attribute Description:	Indicates the measure of survivability of the SNC.
*Type/Syntax:	Enum list • Unprotected, • Single Point of Failure • Diverse • HighlyProtected • Unspecified
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value:	Unspecified

*Invariant?	Y

The following SNC Attributes that are modified:

*Attribute Name:	directionality
Attribute Description:	Specified by NMS by object creation request.
*Type/Syntax:	Enum { bidirectional, unidirectional, point-to-multipoint }
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value	N/A
*Invariant?	Y

*Attribute Name:	protectionLevel
Attribute Description:	Specified by NMS upon object creation Determined based on best effort of EMS to implement requested protection level *commonProtection* is used for 1:N and N:M protection to indicate that protection may not be available when required.
*Type/Syntax:	Enum { protected, preemptible, unprotected, commonProtection }
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value	N/A
*Invariant?	Y

OM.4 TP Object:

The following new operation is added to TP object:

*Operation Name:	getActiveTP
Operation Description:	The operation returns an outTP that is currently passing traffic to or from the inputTP. For MS Linear and equipment protection the input is the source CTP and the output is the active TP. For BLSR the input is the source CTP and the output is the active CTP. For SNCP the input is the sink CTP (that performs the switch) and the output is the CTP that is transmitting to that CTP.
Precondition(s):	The TP is connected in an SNC.
*Parameter Name(s):	inTP
Parameter Description(s):	inTP is the TP that is queried to determine the current transmission path used by that TP.
*Parameter Type(s):	
Return Type Description(s):	outTP
*Return Type/Syntax:	TP
Postcondition(s):	
*Operation	• operation is not supported for this

Exception(s):	object. (This is the case where the TP is not part of an active cross connect.)

OM.5 TPPlan Object

The following new attribute will be added to TPPlan:

*Attribute Name:	protectionType
Attribute Description:	List of attribute id-value pairs representing the transmission parameters for the termination point.
*Type/Syntax:	enum { Both, MainOnly, ProtOnly} "MainOnly" is used for for main of protected SNC. "ProtOnly" is used for protection path of protected SNC "Both" is used when a TP is common for main and protection routes or the TP is unprotected. "Other" is used when unknown or not applicable.
Readable by NMS?	Y
*Writeable by NMS?	N
Default Value	Both
*Invariant?	Y

Fig. 6 illustrates an embodiment of the present invention wherein the main (working) path is determined according to the shortest path found in the network. This main path is described in the Figure as a broken line **a**.

Fig. 7 illustrates an example of another embodiment of the present invention wherein the main (working) path is determined according to the switch default (rather than active) position in the network. Again this main path is described in the Figure as a broken line **a**. Also, as may be seen in this Fig. One preferred way of determining a main path (either according to this embodiment or according to that presented in Fig. 6) is by defining the path to start at the receiving end, and defining the path backwards, toward the transmitting end of the network. Also, the main (working) path can be determined according to the switch initial position in the network.

Fig. 8 demonstrates a further embodiment of the invention wherein the network has a nested intra-layer protection architecture, and the example presented in this Fig. demonstrates a protective path that is in both the optical layer and the MS layer and comprises a number of segments.

It will be appreciated that the above described methods may be varied in many ways, including but not limited to, changing the exact implementation used. It should also be appreciated that the above described description of methods and networks are to be interpreted as including network in which the methods are carried out and methods of using the network components.

The present invention has been described using non-limiting detailed descriptions of preferred embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. It should be understood that features described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all the features shown in a particular figure. Variations of embodiments described will occur to persons of the art. Furthermore, the terms "comprise", "include",

"have" and their conjugates, shall mean, when used in the claims "including but not necessarily limited to".

Claims

1. A method for managing a multi-layered network wherein a selection criterion is used for determining a main transmission path as distinct from a protective path.

2. A method according to claim 1, wherein said selection criterion is based on the definition of the shortest available transmission path and determining said path as the main path.

3. A method according to claim 1, wherein said selection criterion is based on the position of the various switches located along the available transmission paths and is determined in accordance with the default position of these switches.

4. A method according to any one of claims 1 to 3, wherein said multi-layered network is an SDH network that comprises a at least two different layers each selected from the group consisting of optical channel layer, multiplexed section layer, SDH high order layer and ATM layer.

5. A method according to any one of claims 1 to 3, wherein said multi-layered network is a SONET network that comprises a at least two different layers each selected from the group consisting of optical channel layer, VT layer, STC layer, Section layer, line layer and ATM layer.

6. A method according to any one of claims 3 or 4, wherein said at least two different layers comprising each its own independent protection path.

7. A method according to claim 6, wherein the protective path comprises at least two segments that are not directly connected to each other.

8. A network management element for managing the operation of a multi-layered telecommunication network, operative to determine a main transmission path in the network to be managed as distinct from a protective path therein.

9. A network management element according to claim 9, adapted to operate in an SDH network.

10. A network management element according to claim 9, adapted to operate in a SONET network.

11. A system comprising a network management element characterized in that the main communication transmission path and the protective path are defined at the network level.

12. A method according to Claim 1, substantially as described and exemplified herein with reference to the drawings.

13. A network element according to Claim 9, substantially as described and exemplified herein with reference to the drawings.

For the Applicants,

By:

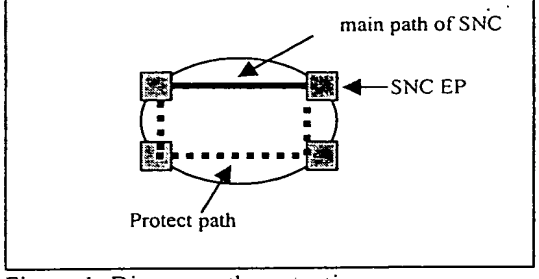

Figure 1. Diverse path protection

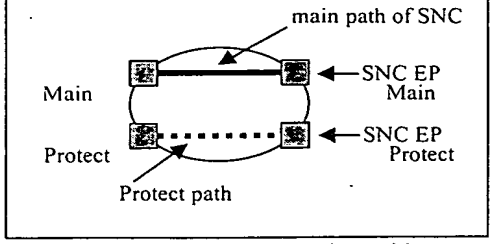

Figure 2. Diverse path protection without common endpoints

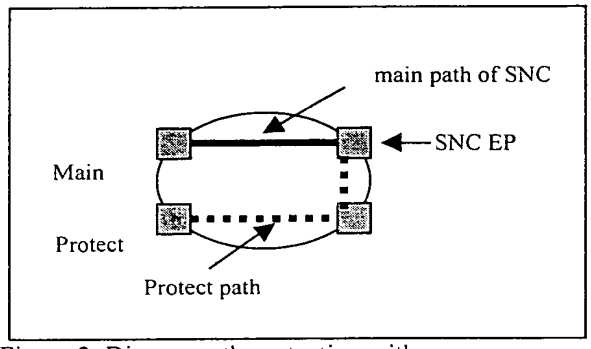

Figure 3. Diverse path protection with one common endpoint

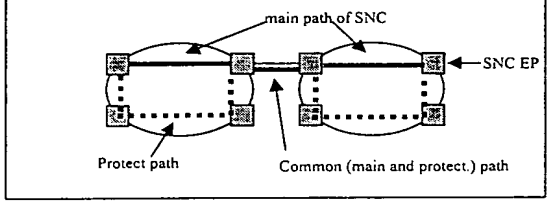

Figure 4. Single point of Failure

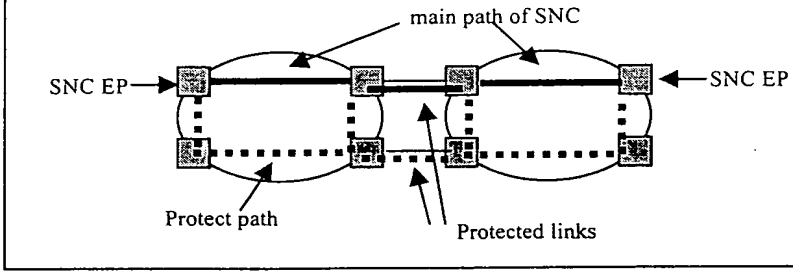

Figure 5. Dual Ring Interworking (DRI).

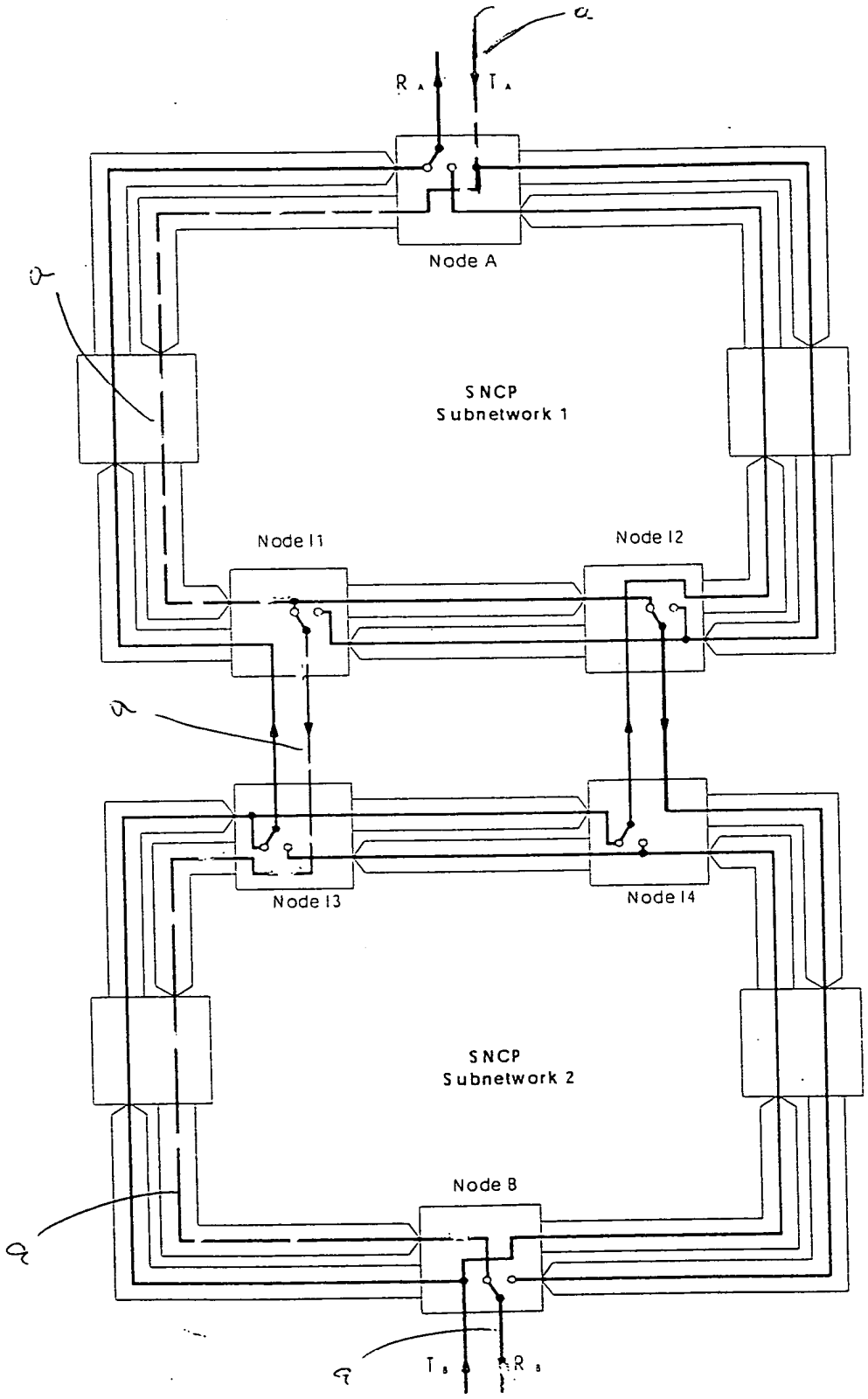
a
R_A
T_A
Node A
SNCP
Subnetwork 1
Node I1
Node I2
Node I3
Node I4
SNCP
Subnetwork 2
Node B
T_B
R_B

Fig 6

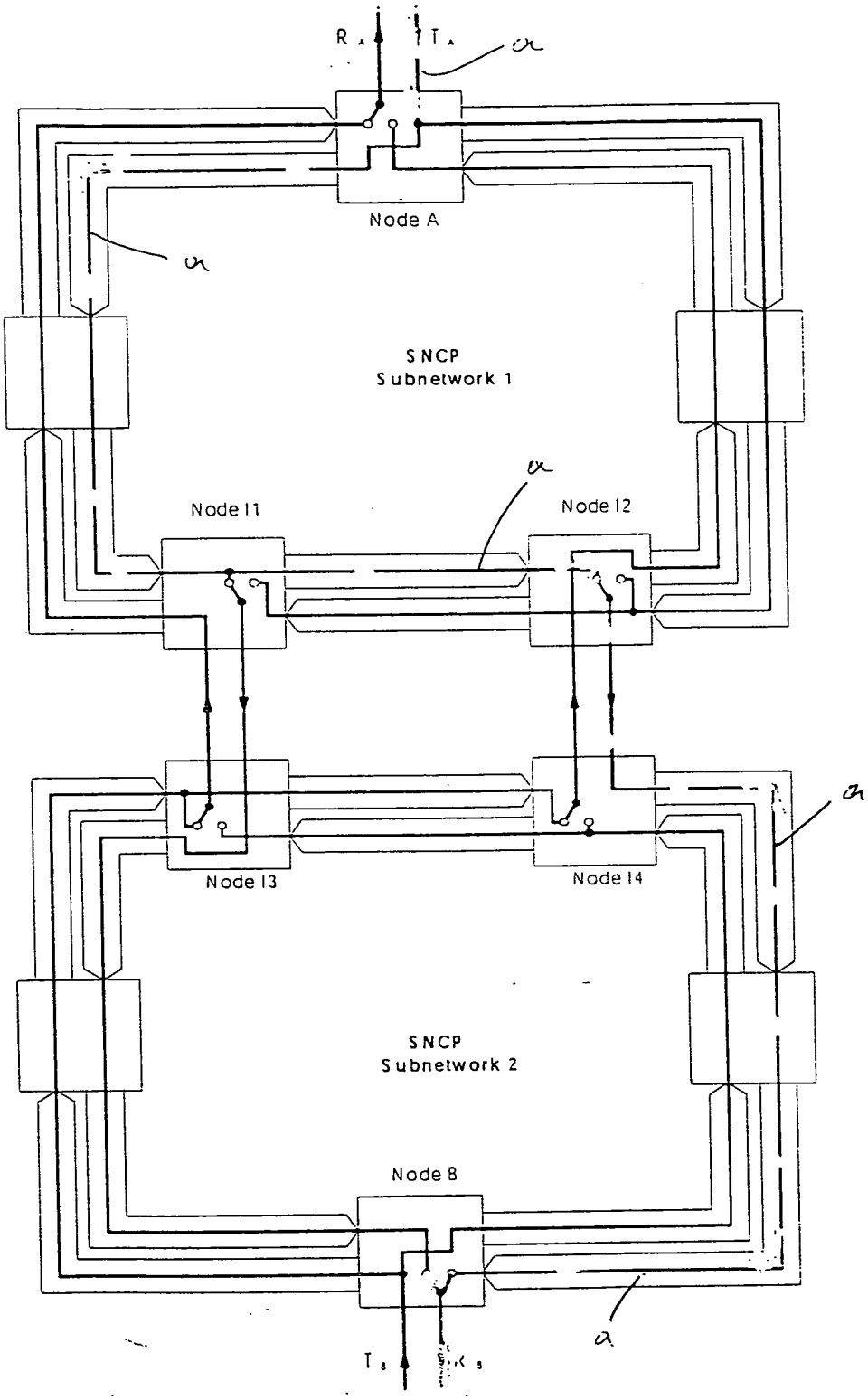
R A
T A
Node A
SNCP
Subnetwork 1
Node I1
Node I2
Node I3
Node I4
SNCP
Subnetwork 2
Node B
T B
R B

Fig 7

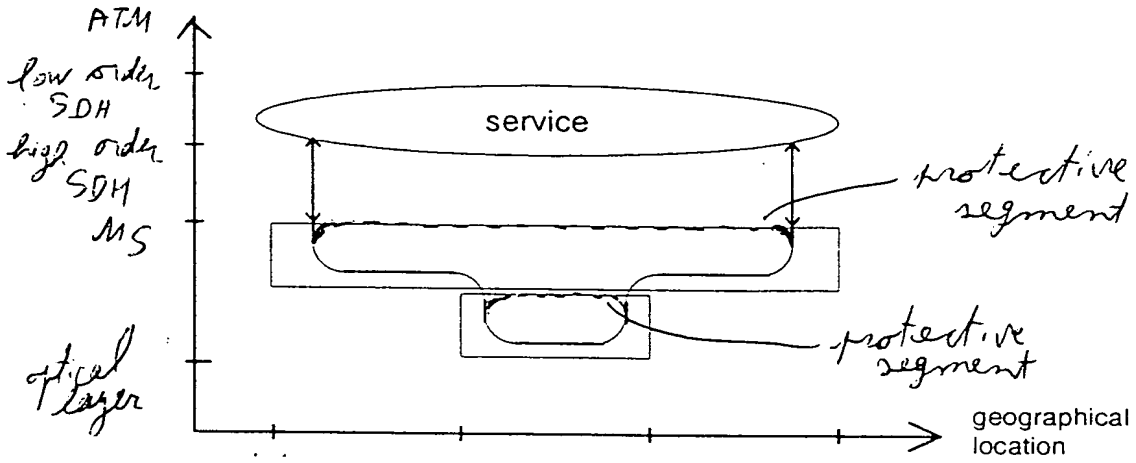
ATM
low order SDH
high order SDH
MS
optical layer
service
protective segment
protective segment
geographical location

Fig. 8